Aspectos Jurídicos da Ciberguerra como Proeminente Modalidade de Conflito Internacional do Século XXI

Laiane Aparecida Dantas de Oliveira[1]
Débora Coelho dos Santos[2]
Maria Eduarda Wandebildes Pita Leite[3]
Maria Luiza Lacerda Bittencourt[4]
Matheus Henrique da Cunha Gomes[5]
Nara Nathália Rosa Maia[6]

Área temática: O Direito Internacional e os conflitos armados do século XXI

RESUMO

No presente artigo buscou-se investigar os efeitos dos conflitos cibernéticos nas relações internacionais entre os Estados como relevante modalidade de conflito internacional no século XXI. Para alcançar o objetivo proposto, foram utilizadas fontes predominantemente teóricas, em uma abordagem compreensivo-exploratória e histórico-reflexiva sobre a matéria, no qual será analisado, a partir do estudo de casos, o tratamento conferido pelo Direito Internacional em relação à denominada ciberguerra. Adotou-se como referencial teórico a "Teoria do Uso da Força" em análise sobre os conflitos cibernéticos com maior destaque nos últimos anos Como resultados, será exposto que os instrumentos tradicionais de repúdio ao uso da força são insuficientes para a prevenção e repressão à ciberguerra, exigindo a instituição de novas estratégias de defesa para a proteção de informações presentes em *softwares* e infraestruturas de *hardware* dos Estados. Ao final, propõe-se a elaboração de tratado internacional para positivar e orientar a conduta dos sujeitos de Direito Internacional acerca dos conflitos cibernéticos.

Palavras-Chave: Ciberguerra; Uso da Força; Novas Ameaças; Soberania.

---

[1] Advogada. Mestranda e Estagiária Docente do Programa de Pós-graduação Stricto Sensu em Direito da Universidade FUMEC, em Belo Horizonte, Minas Gerais.
[2] Graduanda em Direito pela Universidade FUMEC.
[3] Graduanda em Direito pela Universidade FUMEC.
[4] Graduanda em Direito pela Universidade FUMEC.
[5] Graduando em Direito pela Universidade FUMEC.
[6] Graduanda em Direito pela Universidade FUMEC.

1 INTRODUÇÃO

As revoluções tecnológicas criaram um novo espaço para a sociedade: o Ciberespaço. Desde a descoberta de 'novos' livros bíblicos a ofertas de trabalho esdrúxulas no Craigslist[7] a informação nunca propagou tão rápida a um número tão grande de pessoas. Nesse local, não há barreiras ou limites que não podem ser ultrapassados, tampouco há fronteiras que delimitam o ciberespaço de cada ente internacional sobre o qual incida alguma legislação.

Seja por dolo ou por culpa, as transgressões de conduta no ambiente cibernético são generalizadas e podem provocar danos imensuráveis. Afirma-se, portanto, que, nesse espaço, os atos praticados por um usuário que vão ao encontro de outrem não são todos considerados ataques, cabe à Teoria do Uso da Força determinar aquilo a ser considerado como tal, passando a ser conhecido então como ciberameaça. É também de acordo com essa teoria que se designa o ponto a partir do qual a ameaça cibernética se torna guerra cibernética.

Partindo dessas linhas introdutórias, a problemática apontada consiste nos efeitos decorrentes da ciberguerra no contexto internacional. A investigação se dá em virtude da necessidade de produção de estudos analisando incidentes cibernéticos conflituosos, com seus respectivos efeitos jurídicos e sobre o aspecto da segurança internacional. Partindo de uma perspectiva histórica envolvendo diálogos entre o Direito Internacional Público, o uso da força e a segurança internacional, o objetivo do presente trabalho é investigar e demonstrar a consequência dos conflitos relatados sob o aspecto jurídico social internacional.

A metodologia de pesquisa adotada foi documental e bibliográfica, analisando os textos especializados, com destaque para a doutrina especializada, os instrumentos convencionais e os estudos de casos. Para alcançar o objetivo proposto, utilizar-se-á de fontes predominantemente teóricas, em uma abordagem compreensivo-exploratória e crítico-reflexiva sobre a matéria.

2 SOCIEDADE EM REDE: EVOLUÇÃO DA SOCIEDADE SOB A INOVAÇÃO TECNOLÓGICA

Atualmente a sociedade se depara com um avanço acelerado da tecnologia em suas diversas formas de atuação, estando presente em todos os momentos da vida das pessoas. É possível ter acesso a outras culturas, paisagens, políticas, esportes e diversos assuntos ocorridos em qualquer lugar do mundo, sem ter que sair de casa. Tudo isso pode ser transmitido, reproduzido e repassado para milhões de pessoas bastando apenas um clique.

Para FLORÃO (2006):

> O crescimento da interdependência entre os povos e países da superfície terrestre, que alguns preferem denominar de 'Aldeia Global', pois parece que o Planeta está ficando menor, e todos parecem se conhecer (assistem a programas de televisão, ou através da Internet, ficam sabendo o que ocorre no mundo todo, no mesmo dia, e muitas vezes, no ato do conhecimento), se deve ao enorme desenvolvimento nos

[7] Cragslist promove classificados e fóruns locais para empregos, imóveis, vendas, personals, prestação de serviços, comunidade local e eventos (cragslist.org)

> meios de transporte, comunicação, nas viagens e no turismo internacional, nas trocas comerciais entre os países.

Faz-se importante trazer um breve panorama histórico a respeito das revoluções tecnológicas existentes até os dias atuais. De acordo com Alvin Toffler, existiram até hoje três tipos de revoluções tecnológicas: a agrícola, a Revolução Industrial e a digital. (TOFFLER, 1980 p. 35 et seq).

De acordo com Luis Magalhães, a primeira revolução tecnológica, caracterizada pela substituição de ferramentas manuais por máquinas, ocorreu ao final do século XVIII, com a introdução de novas tecnologias como a máquina a vapor, o tear mecânico e a metalurgia.

A segunda revolução, que foi marcada pela eletricidade, ocorreu na parte final do sec. XIX, com novas tecnologias como produção, transporte e utilização da eletricidade, a química industrial, a laminagem e moldagem do aço, o motor de combustão interna, o telégrafo, e o telefone.

A terceira revolução tecnológica se iniciou na 2ª Guerra Mundial com o computador programável em 1946, o transistor em 1947 e o circuito integrado em 1957. Conduto, ela se afirmou por volta de 1970, com o interruptor digital e as redes de computadores em 1969, a fibra óptica de comunicação e o microprocessador em 1971. A interação entre computadores, baseada em ícones e no mouse e a Internet em 1973, com destaque para os avanços ocorridos em 1990 através da conjugação das plataformas cibernéticas nos aparelhos celulares. “Esta última revolução é denominada como tecnologias da informação e da comunicação”. (MAGALHÃES, 2001).

Desde o fim dos anos 90, as mudanças tecnológicas vêm ocorrendo de uma forma exacerbada e foi a evolução dos sistemas de informação que contribuiu consideravelmente para este cenário, tendo como consequência uma acentuada mudança em toda a sociedade, tanto no âmbito interno, como no âmbito internacional.

Internamente as pessoas adquiriram ferramentas que além de facilitar a vida quotidiana, proporcionam também maior participação da sociedade como um todo ou individualmente que por esses meios possuem maior facilidade para expressarem suas opiniões políticas, ideológicas, religiosas de uma forma mais abrangente, alcançando maior número de pessoas.

Devido à facilidade de comunicação, que ocorreu principalmente pela internet, foram surgindo várias formas de interação que interligam cada vez mais os indivíduos e também as sociedades de diferentes culturas, através de seus sons, imagens, e ferramentas digitais.

Toda essa estrutura é denominada, por Manuel Castells, como ‘Sociedade em Rede’ que pode ser definida como uma sociabilidade assente numa dimensão virtual, possível e impulsionada pelas novas tecnologias, que transcende o tempo e o espaço. (CASTELLS, 2002). O que proporciona a existência dessa sociedade é o suporte digital.

Para compreender melhor a Sociedade em Rede se faz necessário um novo conceito de espaço: o espaço virtual/ciberespaço. Nele as barreiras físicas se tornam irrelevantes, formando assim o que Marshall Macluhan apelidou de uma aldeia à escala global. Em decorrência de toda essa evolução originou-se a ciberguerra ou guerra cibernética. Onde não são necessários conflitos ou armas físicas, pois, ela ocorre inteiramente no ciberespaço através da rede, podendo desestabilizar todo um sistema de defesa de um país.

Entretanto, não se pode achar que a tecnologia determina a sociedade, e nem que a tecnologia advém da sociedade. O que acontece é que a tecnologia é a sociedade e a sociedade não pode ser entendida ou representada sem suas ferramentas tecnológicas (BIJKER et al., 1987).

Embora a sociedade não seja determinante para a tecnologia, ainda assim ela pode influenciar diretamente por meio da intervenção do Estado, uma vez que este pode investir em tecnologia, trazendo benefícios a todos, influenciando a economia, o poder militar e o ambiente social (CASTELLS, Manuel). Do mesmo modo que a tecnologia passa por transformações ela também transforma, a todo tempo, o comportamento de uma sociedade, alterando seus hábitos, costumes, linguagens, formas de comunicação, dentre outros.

Atualmente a tecnologia se tornou um instrumento para algo bastante valioso que é o acesso à informação. Os governos investem bastante no desenvolvimento tecnológico de seus países, sendo poucos os detentores das principais indústrias de tecnologias de ponta. Esta postura é compreendida pelo interesse ao poder e ao domínio que o avanço tecnológico pode trazer a um Estado. Como a sociedade em rede possui um condão facilitador, é necessário que os estados estejam preparados para prevenir invasões em seus sistemas de defesa. Dessa forma fica claro que um dos grandes fatores motivadores para o interesse estatal em pesquisa e tecnologia é: prevenir a ciberguerra.

3 A CIBERGUERRA

3.1 SOBRE A CIBERGUERRA

Segundo André Melo Carvalhais Dutra[8], não existe consenso sobre o conceito de ciberguerra, utilizar-se-á aqui a definição de Parks e Duggan[9]:

> Guerra Cibernética é o subconjunto da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra Cibernética é a Internet e as redes a ela relacionadas, as quais compartilham mídia com a Internet.

Apontada como uma nova modalidade de guerra, a ciberguerra tem a capacidade de afetar diretamente os Estados, inclusive no âmbito interno, colocando em cheque os princípios inquestionáveis como a Soberania, por exemplo.

A guerra cibernética proporciona meios que facilitam a espionagem podendo ser instrumento na obtenção de diversas vantagens, tais como a obtenção de informações sigilosas de determinado Estado, acesso os meios de combate de Governos opositores em casos de guerras físicas, ou até mesmo na sabotagem de meios de comunicação, tendo a capacidade de afetar diretamente o meio físico causando grandes consequências à estrutura critica como usinas, rede elétrica, sistemas operacionais urbanos, entre outros.

É de grande importância a análise alguns aspectos, como princípios ou indícios, para que atos praticados no espaço cibernético sejam considerados atos típicos de uma ciberguerra. Deve-se analisar se de fato o ato praticado no espaço cibernético veio a causar consequências no mundo físico, acarretando prejuízos a outro Estado. Um segundo elemento essencial é a

---

[8] JOYNER, Christopher C. e LOTRIONTE, Catherine. Information Warfare as International Coercion: Elements of a Legal Framework. Ejil, 2001.

[9] PARKS, Raymon C.; DUGGAN, David P. Principles of Cyber-warfare. Proceedings of the IEEE Workshop on Information Assurance, West Point, NY, p 122 – 125.

identificação do autor deste ato, entretanto nem sempre essa identificação é possível, ainda que atos praticados no espaço cibernético deixem rastros devido a utilização de programas e servidores, existem meios de manipulação e disfarce, que ocultado a autoria, eximindo-a assim de qualquer responsabilização.

A imprevisibilidade é outro fator de extrema importância, tendo em vista que os meios empregados, assim como os equipamentos utilizados em determinado ato são suscetíveis de falhas, podendo intervir diretamente nos resultados. É valido dizer que todo ato praticado no espaço cibernético é controlado por seres humanos através de meios virtuais criados por estes, sendo assim, só é necessário que o autor recorra a forma que lhe convir para realizar os ataques desejados, sendo que as armas utilizadas no mundo virtual não são definidas como as utilizadas nos conflitos armados no mundo físico, a mesma ferramenta utilizada para obter informações de um inimigo pode ser utilizada para solucionar possíveis falhas no sistema, tornando assim o conflito no mundo virtual bastante complexo.

O grande problema da ciberguerra é a má utilização da Teoria Uso da Força constituída até o momento, o que impede em um primeiro momento, a utilização de armas de um Estado atacado virtualmente por outro. Isso se deve principalmente pela dificuldade na identificação impossibilitando a imputação ao Estado autor. Outro fator a ser levado em consideração se trata de quais seriam as providências cabíveis pelo Estado vitimado, tendo em vista que ataques cibernéticos podem gerar prejuízos enormes inclusive na própria infraestrutura básica dos Estados. Entretanto uma solução adequada não foi atribuída pelo Direito Internacional. Semelhante a uma guerra física, a ciberguerra é marcada pela busca à predominância de um Estado em relação ao outro, onde o Estado que melhor se preparar tecnologicamente obtém maior vantagem tanto atacando, quanto se defendendo, sendo que no espaço cibernético as fronteiras são reduzidas e as informações são obtidas instantaneamente.

A Guerra Tradicional é baseada em território e Soberania, entretanto na ciberguerra é impossível definir os limites da soberania de cada Estado no mundo virtual, entretanto, problemas como este devem ser sanados através de novas metodologias visando a preservação da paz mundial bem como a segurança internacional, assegurando a Soberania de cada Estado.

Richard A. Clarke e Robert K. Knake (2010) definem ciberguerra da seguinte maneira:

> É a penetração não autorizada, em nome ou em apoio de um governo de outra nação computador ou rede, ou qualquer outra atividade que afeta um sistema de computador, no qual o objetivo é adicionar, alterar ou falsificar dados ou causar o rompimento ou danos a um computador, ou dispositivo de rede, ou os objetos de controles do sistema de computador. (CLARKE; KNAKE, 2010, p. 228, tradução: Ramos, Maria Sharlyany Marques). [10]

Segundo o professor Joseph Nye, “o termo ‘ataque cibernético’ abrange uma ampla variedade de ações, que vão de simples tentativas para apagar dados até danos a websites, negação de serviço, espionagem e destruição”. (NYE, 2012). Sendo que os obstáculos ao acesso ao campo cibernético são tão irrisórios que grupos não estatais e pequenos Estados

---

[10] “It unauthorized penetration, on behalf or in support of a government in another computer or network nation, or any other activity that affects a computer system, in which the goal is to add, alter or falsify data or cause disruption or damage to a computer or network device, or controls the computer system objects”. (CLARKE; KNAKE, 2010, p. 228)

podem assumir um papel central e a um custo muito baixo. (NYE, 2012). Bernardo Wahl G. de Araújo Jorge diz que “a nova revolução da informação está mudando a natureza do poder e aumentando a sua difusão”.

Muitos especialistas definem ciberguerra como “guerra sem sangue”, pois consiste em um conflito unicamente virtual, entretanto vemos claramente que essa não é a realidade, as consequências geradas no espaço virtual acabam impactando o espaço físico também, como por exemplo, o ocorrido com o programa nuclear Iraniano, o qual foi comprometido através de um vírus altamente destrutível. Chatfield afirmou que “se quisermos conviver com a tecnologia da melhor forma possível, precisamos reconhecer que o que importa, acima de tudo, não são os dispositivos individuais que utilizamos, mas as experiências humanas que eles são capazes de criar”. (CHATFIELD, como viver na era digital, p.15)

3.2 A CIBERGUERRA E A SOCIEDADE EM REDE: CIBERESPAÇO

Não há como falarmos sobre ciberguerra sem compreendermos o espaço onde este fenômeno ocorre, o chamado Ciberespaço. Criado em 1984 por Wiliam Gibson em seu romance de ficção científica Neuromante, o termo ciberespaço era utilizado para descrever o universo das redes digitais, sendo imediatamente retornado pelos usuários e criadores de redes digitais ganhando uma enorme proporção, o que o torna muito prestigiado nos dias atuais. (LÉVI, 1999).

Muito abordado no meio tecnológico o ciberespaço vai muito além de uma simples conexão com a internet, trata-se de um termo bastante amplo envolvendo toda infraestrutura telemática, bem como seu conjunto de informações e os seres humanos envolvidos neste meio de comunicação. Segundo Pierre Lévy, “ciberespaço (também denominado por ele como ”rede”) é o meio de comunicação que surge da interconexão mundial dos computadores”. (LÉVI, Pierre, 1999, p.17). Lévy diz ainda que “o termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo”. (LÉVI, Pierre, 1999, p.17). Neste mesmo sentido Lúcia Leão:

> Camaleônico, elástico, ubíquo e irreversível, o ciberespaço não se reduz a definições rápidas. Partindo de um olhar tríplice, percebemos que o ciberespaço engloba: as redes de computadores interligadas no planeta (incluindo seus documentos, programas e dados); as pessoas, grupos e instituições que participam dessa interconectividade e, finalmente, o espaço (virtual, social, informacional, cultural e comunitário) que emerge das inter-relações homens-documentos-máquinas. (LEÃO, 2004, P.9).

Atualmente, vivemos na era digital, onde a maior parte da sociedade passa a depender plenamente desse ciberespaço, a rede passa a ser elemento essencial não só na vida social, mas também na vida profissional da maioria dos seres humanos. Manuel Castells diz que “na era da informação, as funções e os processos dominantes na sociedade estão cada vez mais organizados em rede”. (CASTELLS, 1999). Walter Clayton de Oliveira, em sua tese de Doutorado em Ciência da Informação:

> Estamos na aldeia global da informação, nos trilhos das vias de comunicação não de átomos, mas de bits, no percurso das sociedades modernizadas, fruto da atual e irreversível tendência das relações humanas e sociais para a virtualidade, em que a existência se canaliza e se arrasta vertiginosamente para outros redimensionamentos e, também, para outras problematizações. (OLIVEIRA, Walter Clayton, Tese de doutorado, p.17)

Estamos diante de uma economia informacional, global e em rede, o que possibilita o alcance em escala global de produtividade e competitividade através do ciberespaço devido a revolução da tecnologia da informação. (CASTTELS, 1999).

Essa revolução tecnológica fez com que empresas e até mesmo os Estados passassem a depender do uso da tecnologia, utilizando cada vez mais essa rede, gerando assim uma maior eficiência e grandes reduções de custos, onde processos que anteriormente eram feitos através de mãos humanas foram substituídos, semelhantemente ao ocorrido na revolução industrial, sendo dessa vez, sucedidos por softwares, máquinas e até mesmo pelo uso do ciberespaço. Casttels afirma que "as redes constituem a nova morfologia social de nossas sociedades e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura". (CASTTELS, 1999).

A grande ascensão da tecnologia da informação veio acompanhada de riscos, conforme diz José Pedro Teixeira Fernandes:

> O progresso tecnológico que permitiu a sociedade em rede – com todos os imensos benefícios que daí resultaram –, trouxe consigo uma nova área de risco para as sociedades humanas, consequência paradoxal (inevitável?) do seu sucesso. Para além das possibilidades de extorsão financeira, de vendas fraudulentas, de pornografia infantil, etc. – que cabem no âmbito das infrações legais e/ou criminalidade –, surgiram também possibilidades adicionais de difusão de ideologias políticas radicais e violentas e, aspeto de risco inteiramente novo, uma possibilidade de os conflitos internacionais decorrerem no ciberespaço, em paralelo, ou não, com uma guerra física (cinética). Paradoxalmente, esta nova possibilidade que, num cenário extremo, poderá ser imensamente destrutiva, só se tornou possível pelos avanços tecnológicos da sociedade em rede. Indubitavelmente, estamos perante mais um risco da atual modernidade reflexiva. (FERNANDES, José Pedro Teixeira, 2013).

No cenário atual, o mundo se movimenta através da rede, a velocidade de fluxo de informações e a praticidade adquirida com o avanço tecnológico fizeram com que a maior parte das empresas e até mesmo os Estados, passassem a armazenar dados, informações e serviços, inclusive sigilosos, nesse ciberespaço através de computadores e servidores. Vê-se de forma clara essa realidade, onde uma empresa tem a possibilidade armazenar dados de seus funcionários e clientes em computadores ou servidores, ou de um cliente ter acesso à sua conta bancaria pessoal através de um terminal, computador ou smartphone, até o armazenamento de projetos nucleares de Governos no denominado ciberespaço, o que faz com que os riscos atrelados à ascensão tecnológica sejam cada vez mais iminentes.

De fato, o ciberespaço proporciona grandes vantagens, a diminuição das barreiras e a velocidade com que se tem acesso às informações são incríveis, o que pode trazer vários benefícios, não só para os Estados, mas também para toda sociedade. Entretanto se for usado de forma inapropriada pode sim trazer consigo consequências desastrosas não apenas no mundo virtual, mas também no mundo físico, comprometendo inclusive a paz e a segurança

internacional. Cabe assim cada Estado a usar de maneira benéfica e responsável esse mundo fascinante chamado Ciberespaço.

4 O USO DA FORÇA E A CIBERGUERRA – TEORIA DO USO DA FORÇA

Desde os primórdios, o uso da força é tido como meio para demonstrar domínio e poder nas relações humanas, primeiramente no intuito de defesa individual e posteriormente dado a formação dos primeiros clãs e comunidades, para a defesa coletiva. Ocorre que com o surgimento dos Estados, bem como o avanço da sociedade, onde há o enaltecimento do patriotismo, o uso da força tornou-se o Uso instrumento de proteção da Nação e o Direito à Guerra, *jus ad bellum* inerente.

Em 1945, a Organização das Nações Unidas, instituição criada após os escombros deixados pela Segunda Guerra Mundial, aprovou a Carta das Nações Unidas que continha um modelo de conduta a ser seguido pelos Estados-membros, assim não somente aboliu permanentemente a guerra como recurso lícito, mas passou a usar o termo "Uso da Força", ampliando a restrição a qualquer tipo de investida armada, e promovendo a ideia de 'Segurança Internacional' e 'Manutenção da Paz' como fundamentais ao progresso da humanidade.

Com o tempo, o *jus ad bellum* "o chamado direito à guerra, o direito de fazer a guerra quando esta parecesse justa" [11] foi deixado de lado, visando a manutenção da paz, da segurança internacional e especialmente na proteção dos direitos humanos e fundamentais.

A referida Carta traz em seu artigo 2º: Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas. [12]

Na carta, o termo "guerra" é substituído pelo "uso da força". Nesse aspecto, o *jus ad bellum* perdeu espaço para o *jus contra bellum* que é o direito da prevenção à guerra. A guerra somente é considerada lícita ou justa aos Estados em duas exceções: a legítima defesa contra conflito armado e a hipótese de luta de autodeterminação de um povo.

Assim sendo, é possível fazer uso da força numa ciberguerra de forma lícita e dentro das leis que o Direito Internacional oferece, uma vez que estas foram redigidas antes da própria internet ou há uma "área cinzenta" nessa lacuna?

É de competência do órgão da ONU autorizar, quando julgarem necessário, o uso de medidas nesses casos: artigo 39. O Conselho de Segurança determinará a existência de qualquer ameaça à paz, ruptura da paz ou ato de agressão, e fará recomendações ou decidirá que medidas deverão ser tomadas de acordo com os Artigos 41 e 42, a fim de manter ou restabelecer a paz e a segurança internacional.

David Graham diz: "A maioria das decisões apenas chegam após extensas e morosas deliberações, e, mesmo então, estão sujeitas ao veto de qualquer um dos membros permanentes do Conselho de Segurança. Assim, dada a natureza nebulosa e com nuances dos ciberataques e a incerteza de saber como o Conselho de Segurança responderá aos mesmos de forma atempada, parece válido assumir que um Estado escolherá lidar com os ciberataques através do exercício do seu direito de legítima defesa".

---

[11]REZEK, José Francisco – Direito Internacional Público: Curso Elementar, 15ª Edição.
[12] Carta das Nações Unidas - http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm

Devido a esse lapso temporal que pode prejudicar as vítimas de um ciberataque, uma via que vem recentemente sendo utilizada pelos Estados é a tentativa de equiparação de ciberataques aos conflitos armados, pois só assim, poderão se utilizar a legitima defesa e do uso da força (desde que pautada pela proporcionalidade e em resposta a um ataque já existente) em benefício da proteção de seus dados, informações, rede e/ou computadores.

Portanto, a legítima defesa só se configura quando o Estado reage a agressão injusta, atual ou iminente por parte de outro Estado que utiliza a força de forma injusta (não reconhecida/autorizada pelo Direito Internacional Público), devendo esta resposta ser proporcional ao ataque, comunicando-se imediatamente o ato ao Conselho de Segurança da ONU.

O termo "ataque armado" possui definição doutrinária, segundo o jurista Jean Pictet "o uso da força será considerado um ataque armado quando passar o teste do escopo, duração e intensidade suficiente.". Apesar de divergências quanto a esse conceito, foram apresentados três modelos que pretendem "facilitar os critérios do uso da força de Pictet – escopo, duração e intensidade – aplicando-os a formas não convencionais de uso da força, incluindo ciberataques." [13].

O primeiro modelo baseia-se em uma abordagem instrumental (instrument-based approach), e a partir dele é feita uma avaliação para saber se o dano provindo do ataque poderia ter sido causado apenas por um ataque cinético. Essa qualificação se relaciona com o fato de um ataque a uma rede elétrica, por exemplo, antes da cibercapacidade, requerer um bombardeamento ou algum tipo de força cinética para sua execução.

O segundo modelo tem sua abordagem baseada nos efeitos (effects-based approach) ou consequências, esse modelo fundamenta-se no efeito global que o ciberataque tem para os Estados e suas vítimas. Por exemplo, a manipulação de dados e informações de instituições financeiras pode ser equiparado a um ataque armado, uma vez que impactará no bem-estar econômico da vítima.

O último modelo se baseia na responsabilidade estrita (strict liability), sendo assim, qualquer ataque a qualquer infraestrutura nacional seria equiparado a um ataque armado, por causa das rigorosas consequências que tal investida pode resultar.

Ainda com divergências, é certo de que os ciberataques podem se equivaler a ataques armados. Para melhor elucidar esse conceito, Michael N. Schmitt[14] desenvolveu seis requisitos para ponderar em que grau esse nivelamento ocorre:

> (i) gravidade (severity): os ataques armados ameaçam danos físicos e destruição da propriedade num grau muito mais elevado que outras formas de coerção;
> (ii) iminência (immediacy): as consequências negativas de uma ação armada ou as ameaças das mesmas geralmente ocorrem com mais rapidez do que outras formas de coerção
> (iii) carácter direto (directness): as consequências de uma coerção armada estão mais diretamente ligadas ao *actus reus* (ato de culpabilidade), do que outras formas de coerção que dependem de vários fatores para atuar
> (iv) carácter invasor (invasivness): na coerção aramada, o ato que provoca danos normalmente traduz-se num atravessar da fronteira nacional, enquanto que os atos de guerra econômica geralmente ocorrem fora das suas fronteiras;
> (v) mensuralidade ou extensão (measurability): enquanto que as consequências de uma ação aramada são geralmente fáceis de verificar (por exemplo, um certo nível

[13] David Graham, idem, p. 91.
[14] Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, pp. 18-19.

> de destruição), as consequências de outras formas de coerção são mais difíceis de definição;
> (vi) presumível legitimidade (presumptive legitimacy): na maioria dos casos o uso da força, seja sob o prisma da lei doméstica o da lei internacional, é presumivelmente ilegal, exceto se estivermos perante uma disposição que a permita.

Entretanto, surgiu uma nova discussão em relação ao Uso da Força no âmbito internacional após os atentados de 11 de Setembro de 2001, visto que os Estados Unidos da América ao responder a estes ataques e invadir o Iraque não recebeu autorização do Conselho de Segurança da ONU, tampouco satisfizeram os requisitos da legítima defesa, instituindo assim a "Teoria da Legítima Defesa Preventiva", tema que permanece em discussão por ser considerada por muitos internacionalistas como ilegal. A tensão existe entre os Estados é permanente e os modos pelos quais são buscadas a soluções pra conflitos se transformam a qualquer momento. Isso nos demonstra a constante mutação e desenvolvimento das teorias que mediam o Direito Internacional, no aspecto do Uso da Força principalmente.

É possível que sob a ótica de uma ciberguerra seja lícito o uso da força. Juntamente do avanço da alta tecnologia e o acesso irrestrito ao ciberespaço, e a consciência que o mundo vem tomando de que informação é poder, os Estados caminham a possibilidade de cada vez mais poderem exercer seu direito de legítima defesa ao enfrentar esse tipo de ataque, sendo essencial que haja essa avaliação entre os modelos e requisitos de nivelamento entre "conflito armado" e "ciberataque".

5. PRINCIPAIS CASOS ENVOLVENDO A CIBERGUERRA

As operações bélicas no espaço cibernético se tornaram um desafio para o Direito Internacional dos Direitos Humanos, uma vez que, nos dias atuais a internet e os sistemas digitais são pertinentes na condução de conflitos armados de uma forma que em décadas passadas era não se considerava. A vista disso, a mídia e a doutrina vem relatando ataques por hackers com ações cada vez mais complexas com o objetivo de prejudicar a operacionalidade digital de governos ou grupos não estatais no campo militar. Desta forma, para melhor compreender a ciberguerra, se faz necessário o estudo dos casos emblemáticos que marcaram esta nova modalidade de conflito armado.

Um deles aconteceu em 2007, na Estônia, país no qual quase todos os serviços e tarefas cotidianas da sociedade estão ligadas à rede da Internet, o que pode aumentar a vulnerabilidade na rede pela criação pontos de acesso mal protegidos e utilizados por usuários despreparados. O ataque teve como principal arma o denominado "DDoS" (distributed denial of servisse, ou distribuição de negação de serviço, em português). Tal estratégia consiste em bombardear o site alvo com diversos pedidos falsos de informações, o que faz com que o site bloqueie até que se cesse o ataque. De acordo com dados da "Arbor Networks Active Threat Level Analysis System", houve pelo menos 128 ataques distintos de DDoS na Estônia contra sítios virtuais do governo local.

Ainda que a guerra tenha sido virtual, o fato que levou a tal violência foi bastante factual. Em 2007, no dia 27 de abril, o governo da Estônia removeu o Soldado de Bronze Tallinn, que estava localizado no centro da cidade Tallin ao lado de uma pequena vala que na época da Segunda Guerra manteve os restos mortais de soldados do Exército Vermelho, foi transferido para o Cemitério Militar de Tallinn. A estátua reconhecida como memorial da Segunda Guerra Mundial, significava a vitória da União Soviética sobre o nazismo e foi construída durante o tempo em que o país estava sobre domínio soviético. Essa decisão foi

considerada polêmica e respondida com violência, uma onda de ataques cibernéticos que danificaram sites governamentais e corporativos na Estônia. Tal conflito foi considerado a primeira guerra no ciberespaço com ataques de grandes repercussões.

Embora não houvesse apresentado nenhuma evidencia conclusiva publicamente, o governo da Estônia aponta a Rússia pelos ataques. Além da retirada da estátua significar para os russos o incentivo a ações nazistas, segundo alguns, a série de ataques cibernéticos foi acionada por ordens originadas da Rússia ou de fontes de etnia russa em retaliação à retirada da estátua. Ademais, estonianos afirmaram que um endereço de internet envolvido nos ataques pertencia a um oficial que operava na administração do presidente da Rússia, Vladimir V. Putin. Dessa forma, especialistas em cibersegurança da OTAN, da União Europeia, dos Estados Unidos e de Israel se reuniram em Tallinn para oferecer ajuda e descobrir o que fazer para lidar com uma guerra cibernética na era digital.

Apesar de esse ser considerado o primeiro evento de ciberguerra, outros ataques cibernéticos já haviam sido detectados, nos quais governos e seus principais fornecedores foram os alvos, em 1998 batizados de “Moonlight maze” e “Solar Sunrise”.

Moonlight maze é o nome atribuído a um inquérito do FBI a respeito de um ataque cibernético que teve como alvo redes restritas do governo dos Estados Unidos. Estes ataques deram início em março de 1998 e foram direcionados a sistemas que continham informações sensíveis, tendo acesso a milhares de documentos, dentre eles, os sistemas do Pentágono da NASA, do Departamento de Energia (DOE) e algumas universidades militares e civis dos Estados Unidos.

De acordo com o Pentágono e o próprio FBI, escala do roubo era literalmente monumental, porque os investigadores reivindicaram que uma cópia impressa dos materiais roubados seria três vezes mais alta do que o monumento de Washington. O ataque fez parte de uma pretensão russa de acessar tecnologia americana. Os ataques cibernéticos foram bem estruturados, disciplinados, direcionados a objetivos específicos, com extenso conhecimento dos sistemas e suas restrições. Especialistas afirmam que é um exemplo de ameaça persistente e avançada mais duradoura da história. De acordo com Richard Clar, a lição aprendida de “Moonlight Maze” é que os Estados Unidos e sociedades ocidentais se tornaram extraordinariamente vulneráveis à invasão e sabotagem de um sistema crítico de computadores.

O “Solar Sunrise” ocorreu em janeiro de 1998, meio a um clima de tensão entre Estados Unidos e Iraque, inspetores de armas americanas foram expulsos do território iraquiano. Esses ataques tiveram como alvo computadores DOD e a cerca de 500 sistemas de computadores pertencentes ao governo e ao setor privado tiveram seu controle conquistado. Ocorreram no momento em que os EUA estava se preparando para provável ação militar contra o Iraque devido a disputas de inspeção de armas da ONU. Os ataques foram generalizados e pareciam vir de sites como Israel, Emirados Árabes Unidos, França, Taiwan e Alemanha.

Usando-se da conhecida vulnerabilidade do sistema operacional e com ajuda de um vírus de computador, pelo menos onze ataques seguiram o mesmo perfil em sistemas da Força Aérea, da Marinha e do Corpo de Fuzileiros Navais em todo o mundo. Em seguida, o Departamento de Defesa tomou medidas extremas a fim de evitar futuros incidentes desse gênero.

Outro acontecimento que merece destaque foi a operação reconhecida como “TiTan Rain”, nome dado pelo Governo Federal dos Estados Unidos para uma série de ataques cibernéticos, que se acredita ter começado em 2003 e seguido até 2007, sendo que somente em 2004 o governo detectou a falha de segurança no seu espaço cibernético. Teve como alvo os fabricantes de armamentos e a NASA, novamente com o intuito de obter informações

importantes e sigilosas. O suspeito pela invasão era o exército chinês a fim de espionar os EUA.

As ameaças de espionagem e obtenção ilícita de informações configuram uma guerra cibernética silenciosa. Mas, apesar do silêncio aparente, os países vêm se organizando e se preparando contra esses ataques na nova ordem mundial.

6 O FUTURO DA CIBERGUERRA

Há 20 anos, Arquilla e Ronfeldt afirmaram que a ciberguerra estava a caminho e poderia impactar a segurança no século XXI de modo significante. Agora, já quase no fim da segunda década do terceiro milênio, a cena em que se encontra é de guerra virtual com resultados tão danosos como se com artilharias e homens frente a linha de batalha. A pergunta é como daqui para frente será o cenário de segurança mundial?

Diante da incerteza de um futuro que promete ser cada vez mais tecnológica, a expansão do ciberespaço é evidente, com a evolução da robótica e com conexão em rede mais rápida. A abrangência do ciberespaço aumenta e as ações nele possíveis são cada vez mais variadas, logo, esse lugar se desenvolve a cada momento de forma descontrola, agravando a vulnerabilidade estrutural e informacional para aqueles se utilizam dele.

Ciente da crescente proporção do uso da cibernética nos conflitos internacionais, o Brasil viu a necessidade de se proteger de modo compatível a sua própria dimensão e suas aspirações político-estratégicas no cenário internacional contra tal ameaça. Para tanto o Estado brasileiro tem criado políticas que delimitam e, de certa forma, diminuem a '‘névoa’' que recepciona a guerra cibernética, justamente por não ser possível e, muitas das vezes, saber que está sendo atacado e qual é o responsável.

Por adotar uma postura internacional de promoção de paz, o Brasil não deve se preocupar em produzir armas cibernéticas ou algo do tipo, mas sim, com a proteção de suas redes. Quanto as possíveis ações ofensivas no ciberespaço que, em tempo de paz, devem limitar-se a desenvolver capacidades para que, ante a inevitabilidade de algum conflito, possam ser eficaz em acelerar a derrota do oponente e restringir os danos de seu esforço ao mínimo possível. Contudo, a politica do ‘peacekeeping’ não é a postura adotada pela maioria dos países. Entre os Estados com capacidades ofensivas, os Estados Unidos, China e Rússia já anunciaram publicamente a existência de unidades de guerra cibernética dentro de suas forças armadas.

Em razão disso, ataques a vários entes e personalidades internacionais como Google, Microsoft e Yahoo foram tema de discussão durante a 71ª Sessão da Assembleia Geral das Nações Unidas. Apesar de ser um órgão governamental global, os esforços da ONU não conseguiram muito na forma de desencorajar ciberataques e ciberguerra em geral.

Mais recente, na Conferencia RSA em São Francisco em 2017, a Microsoft defendeu a ideia de que não são politicas singulares de defesa que vão combater os ataques cibernéticos, mas que “chegou o momento de apelar aos governos do mundo para programar regras internacionais para proteger o uso civil da internet” (tradução livre). De acordo com Brad Smith[15], há a necessidade de uma Convenção de Genebra Digital, pois:

---

[15] Brad Smith é o presidente e diretor jurídico da Microsoft. Smith desempenha um papel fundamental na representação externa da empresa e na liderança do trabalho da empresa em uma série de questões críticas, incluindo privacidade, segurança, acessibilidade, sustentabilidade ambiental e inclusão digital, entre outros.

> “Primeiro, há uma nova oportunidade para ações bilaterais vitais. [...] Em segundo lugar, os governos de todo o mundo devem buscar um acordo multilateral mais amplo que afirme as recentes normas de segurança cibernética como regras globais. [...] Precisamos de uma Convenção Digital de Genebra que comprometa os governos a implementar as normas que foram desenvolvidas para proteger os civis na Internet em tempos de paz. Tal convenção deve comprometer os governos a evitar ataques cibernéticos que visem o setor privado ou infraestrutura crítica ou o uso de hackers para roubar propriedade intelectual. Da mesma forma, deveria exigir que os governos ajudassem os esforços do setor privado para detectar, conter, responder e recuperar desses eventos, e exigir que os governos relatassem vulnerabilidades aos fornecedores em vez de armazená-los, vendê-los ou explorá-los”.

O empresário acrescentou que a partir dessa convenção precisa ser criada uma organização independente formado por membros do setor privado, acadêmico e social, capaz de abranger os setores público e privado que possa investigar e tornar públicas as evidências que atribuem atentados de estados a países específicos.

Acredita-se que o ciberespaço, ainda que com peculiaridades deva ser tratado de acordo com a norma maior vigente de Direito Internacional Público, a Carata das Nações Unidas. A qual rege que o esforço internacional deve ser “preservar as gerações vindouras do flagelo da guerra [seja da modalidade que for]” por meio da tolerância, da paz e da boa vizinhança de um Estado para com o outro.

7 CONCLUSÃO

Diante do exposto, pode-se afirmar que em decorrência do avanço tecnológico surgiu uma nova modalidade de guerra, denominada ciberguerra. Este fenômeno que ocorre no ciberespaço tornou-se uma ameaça real à soberania dos Estados ao redor do mundo, onde mesmo o “Uso da Força” envolvendo práticas internacionais construídas com base na guerra “Tradicional”, é inerente a construção de uma nova teoria que seja capaz de dar resposta adequada pelo Direito Internacional, a fim de que os Estados possam responder a essa nova ameaça objetivando gerar maior segurança internacional.

Após a análise dos exemplos supracitados de ciberguerra, observa-se que foram ameaças persistentes, avançadas e duradouras da história e serviram como alerta para que outros Estados se organizem em uma nova ordem mundial, a fim de superar a vulnerabilidade existente em seus sistemas operacionais e possíveis ataques.

A comunidade internacional, reconhecendo a complexidade e a vulnerabilidade das plataformas virtuais pede a normatização da conduta e, mais que isso, uma diretriz de como combater o mal do ciberespaço, que atinge de forma indiscriminada usuários, Estados e empresas, pelos mais diversos motivos.

Sendo assim a ONU caminha a criar um tratado internacional que honre a sua Carta constituinte, pois no ciberespaço ou não, a prática de guerra deve ser confrontada. E ainda que possibilidade de eliminar completamente a guerra cibernética seja uma ambição praticamente inalcançável a este momento, para um futuro próximo, há uma esperança real de reunir os principais atores para desestimar a situação, conceituando os elementos, positivando normas de conduta para que a convivência no espaço cibernético seja menos hostil.

8 BIBLIOGRAFIA

ARQUILLA, John; RONFELDT, David. *Networks and netwars: The future of terror, crime, and militancy*. Rand Corporation, 2001.

BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de (Orgs.). *Desafios estratégicos para segurança e defesa cibernética*. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. 220 p.

BRASIL. *Doutrina Militar de Defesa Cibernética.* 2014.

BRASIL. *Espionagem Cibernética.* Revista em Discussão. Senado Federal, Ano 5. nº 21. Julho de 2014.

BRASIL. *Estratégia Nacional de Defesa*. Brasília: Ministério da Defesa, 2008.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo. Paz e Terra, 8 ed, 1999.

A Sociedade em Rede. A Era da Informação: Economia Sociedade e Cultura. Volume I. 10ª Edição. 2001.

CHATFIELD, Tom. Como viver na era digital. Rio de Janeiro, Ed. Objetiva, 2012.

CLARKE, Richard A.; KNAKER, Robert K. Cyberwar: *The Next Threat to National Security and What to Do About It*. New York: Ed. Harper Collins. 2010.

CONVENTION ON CYBERCRIME. European Treaty Series - No. 185. 2001.

CRUZ JÚNIOR, Samuel César da. *A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual*. Texto para discussão. Instituto de Pesquisa Econômica Aplicada. Brasília. 2013.

DUTRA, André Melo Carvalhais. *Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto*. São José dos campos. Instituto Tecnológico da Aeronáutica, 4 p. Disponível em: <http://www.sige.ita.br/IX_SIGE/Artigos/GE_39.pdf>. Acessado em: 24 de abril de 2017.

FLORÃO. Santo R. S. *Introdução e Administração: Globalização e Empresa*. Editora Kelps, 3ª Edição. Goiânia. 2006.

GOUVEIA, Jorge Bacelar. O uso da força no Direito Internacional Público. *Revista Brasileira de Estudos Políticos*, nº. 107, pp. 149-200. Belo Horizonte. Jul./dez. 2013. Disponível em:<http://www.pos.direito.ufmg.br/rbep/index.php/rbep/article/viewFile/P.0034-7191.2013v107p149/241>. Acessado em: 24 de abril de 2017.

GROSS, Michael L.; CANETTI, Daphna; VASHDI, Dana Rachel. Cyber Terrorism: Its Effects on Psychological Well Being, Public Confidence and Political Attitudes. 2016.

MAGALHAES, Luis. *Reflexos da evolução científica e das novas tecnologias na sociedade*. Lisboa, 28 de Novembro de 2001. Disponível em: <https://www.math.tecnico.ulisboa.pt/~lmagal/IDN_2.html>. Acessado em: 24 de abril de 2017.

FERNANDES, José Pedro Teixeira. *Da utopia da sociedade em rede à realidade da sociedade de risco*. Análise Social, 207, xlviii (2.º), pp. 260-286. Lisboa, Portugal. 2013.

O Direito Internacional Humanitário e a Emergência da Ciberguerra. *Revista de Direito Internacional, Brasília*, vol. 9, nº 2, jul/dez (2012), pp. 11-24. Disponível em: <http://realpolitikmag.org/wp/index.php/2015/06/05/o-direito-internacional-humanitario-e-a-emergencia-da-ciberguerra/#_ftn30>. Acessado em: 24 de abril de 2017.

JOSEPH, Nye. Guerra e paz no ciberespaço: Ameaças na internet obedecem a uma nova lógica global, São Paulo, 15 de abril de 2012. Disponível em: < http://internacional.estadao.com.br/noticias/geral,guerra-e-paz-no-ciberespaco-imp-,861242>. Acessado em: 24 de abril de 2017.

LEÃO, Lucia. *Derivas: cartografias do ciberespaço*. São Paulo. Annablume, 2004.

LÉVY, Pierre. *Cibercultura*. São Paulo. 34, 1999.

MAULAIS, Cláudio Nunes dos Santos. *Engenharia Social: Técnicas e Estratégias de defesa em ambientes virtuais vulneráveis*. Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento) - Universidade FUMEC, Belo Horizonte. 2016.

MAZZUOLI, Valério de Oliveira. *Curso de Direitos Humanos*, 3 ed. 2016.

MELLO, Selma Ferraz Motta. *Comunicação e organizações na sociedade em rede: novas tensões, mediações e paradigmas*. Dissertação (Mestrado em Ciências da Comunicação) – Universidade de São Paulo, Escola de Comunicações e Artes, São Paulo. 2010.

OLIVEIRA, Walter Clayton. *Ciberespaço, técnica e hermenêutica: Diálogos da ciência da informação*. Tese (Doutorado em Ciência da Informação) – Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, São Paulo. 2013.

OPPERMANN, Daniel. *Governança da Internet e Segurança Cibernética no Brasil*. Monções: Revista de Relações Internacionais da UFGD 2.4, p.259-283, 2014.

RAMOS, Maria Sharlyany Marques. *Ciberguerra e a política de cooperação da UE com a OTAN*. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Roraima, Roraima. 2015.

REZEK, José Francisco. *Direito Internacional Público: Curso Elementar*. Saraiva, 15 ed. 2014.

SALOMÃO, Wiliander França. O uso da força e a legítima defesa permitidos pela ONU. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 16, n. 2956, 5 ago. 2011. Disponível em: <https://jus.com.br/artigos/19706>. Acessado em: 24 abril 2017.

SILVA, Carla Ribeiro Volpini.; ROSA, Patrícia Rodrigues. O uso da força em direito internacional - Legítima defesa preemptiva. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=a08c938c1e7c76d8>. Acessado em 24 de abril de 2017.

SIMTH, Brad. The Need for a Digital Geneva Convention. Transcript of Keynote Address at the RSA Conference. San Francisco, California. 2017.